



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001186122 A**(43) Date of publication of application: **06.07.01**(51) Int. Cl. **H04L 9/32**
G09C 1/00(21) Application number: **11363579**(71) Applicant: **FUJI ELECTRIC CO LTD**(22) Date of filing: **22.12.99**(72) Inventor: **YANAGIHARA HIDEAKI**(54) **AUTHENTICATION SYSTEM AND
AUTHENTICATION METHOD**

(57) Abstract:

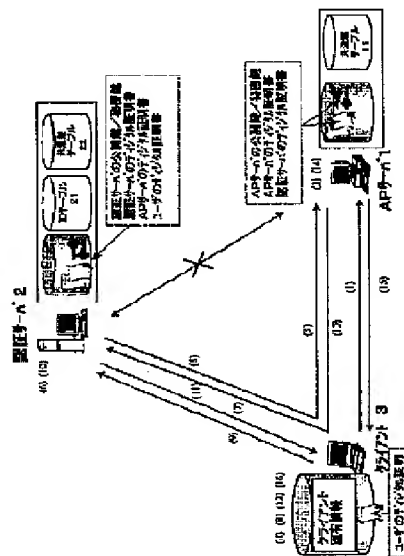
PROBLEM TO BE SOLVED: To provide an authentication system that can prevent leakage of passwords and conduct retransmission of authentication data, by pretending of a 3rd party to be a legal party.

SOLUTION: When a user uses a client 3 to a log in an AP server 1, the AP server 1 generates encrypted communication data (i) and transmits the data as an authentication request to an authentication server 2 by the use of redirection through the client 3. The authentication server 2 makes request to the client 3 to enter its password and authenticates the user, on the basis of the password and the authentication request. Then the server 2 transmits encrypted communication data (iv), including the result of authentication to the AP server 1 by the use of redirection via the client 3. Furthermore, the AP server 1 generates a session ID in the case of log on of the user and registers it to a common key

table 11 with a common key and detects the retransmission by comparing the ID with a session ID in the communication data (iv).

COPYRIGHT: (C)2001,JPO

本実施形態のシステム構成を示す図



【特許請求の範囲】

【請求項1】 クライアントと、認証されたユーザにサービスを提供するアプリケーションサーバ及びユーザの認証を行う認証サーバがネットワークで接続される認証システムにおいて、

前記アプリケーションサーバは、アプリケーションサーバの公開鍵、アプリケーションサーバの秘密鍵及び認証サーバの公開鍵を記憶する第1の記憶手段と、

共通鍵を生成する共通鍵生成手段と、認証対象となっているユーザのクライアントからの接続要求に対し、該クライアントの固有情報を含む認証要求メッセージ及び該認証要求メッセージのメッセージダイジェストを生成するメッセージダイジェスト生成手段と、

前記メッセージを前記共通鍵で、前記メッセージダイジェストを前記アプリケーションサーバの秘密鍵で、及び前記共通鍵を前記認証サーバの公開鍵で暗号化し、これらを認証依頼として前記認証対象となっているユーザのクライアントを介して前記認証サーバに送信する認証依頼送信手段と、

を備え、前記認証サーバは、認証サーバの公開鍵、認証サーバの秘密鍵及びアプリケーションサーバの公開鍵を記憶する第2の記憶手段と、前記認証対象となっているユーザのクライアントを介して受信した前記認証依頼のうち、前記共通鍵を前記認証サーバの秘密鍵で復号化する共通鍵復号化手段と、前記認証依頼のうち、前記共通鍵復号化手段が復号化した共通鍵で前記認証要求メッセージを、及び前記アプリケーションサーバの公開鍵で前記メッセージダイジェストを復号化する復号化手段と、前記復号化手段が復号化した認証要求メッセージから生成したメッセージダイジェストと、前記復号化手段が復号化したメッセージダイジェストを比較して前記認証依頼の改ざんを検出する認証依頼改ざん検出手段と、を備えることを特徴とする認証システム。

【請求項2】 前記認証サーバは、ユーザIDとパスワードを対応させて記憶するアカウント情報記憶手段と、前記改ざん検出手段が前記認証依頼が改ざんされていないと認定した時、前記認証対象となっているユーザのクライアントにパスワードを要求し、該クライアントからパスワードを得るパスワード取得手段と、前記認証要求内のユーザIDと前記パスワード取得手段が取得したパスワードの組合わせが前記アカウント情報記憶手段に記憶されていれば、認証結果として前記ユーザを認証することを示す情報を生成し、該認証結果を含む認証応答メッセージを前記認証依頼に対する応答として前記認証対象となっているユーザのクライアントを介して前記アプリケーションサーバに送信する認証結果送信手段と、を

更に備えることを特徴とする請求項1に記載の認証システム。

【請求項3】 前記認証結果送信手段は、前記認証応答メッセージのメッセージダイジェストを生成し、前記認証応答メッセージを前記共通鍵で、及び前記メッセージダイジェストを前記認証サーバの秘密鍵で暗号化して、これらを前記認証依頼に対する応答として前記認証対象となっているユーザのクライアントを介して前記アプリケーションサーバに送信し、前記アプリケーションサーバは、受信した暗号化された前記認証応答メッセージを前記共通鍵で、及び前記メッセージダイジェストを前記認証サーバの公開鍵で復号化する認証応答復号化手段と、前記認証応答復号化手段が復号化したメッセージダイジェストと、前記認証応答復号化手段が復号化した前記認証応答メッセージから生成したメッセージダイジェストとを比較して前記認証結果メッセージの改ざんを検出する認証依頼改ざん検出手段と、を更に備えることを特徴とする請求項2に記載の認証システム。

【請求項4】 前記アプリケーションサーバは、前記ユーザからのログインに対してセッションIDを生成するセッションID生成手段と、該セッションIDと前記共通鍵を対応させて記憶する第1の共通鍵記憶手段と、前記セッションID生成時に前記共通鍵とセッションIDを前記第1の共通鍵記憶手段に記憶させ、前記認証依頼に対する応答を受信時に、該応答に含まれるセッションIDにより前記第1の共通鍵記憶手段から共通鍵を読み出すと共に該セッションIDと共通鍵を前記第1の共通鍵記憶手段から削除する共通鍵管理手段とを更に備えることを特徴とする請求項1乃至3のいずれか1つに記載の認証システム。

【請求項5】 前記認証要求メッセージは前記セッションIDを含み、前記認証依頼送信手段は、前記認証依頼送信時、前記セッションIDを前記認証対象となっているユーザのクライアントに記憶させ、前記認証サーバは、前記セッションIDと前記共通鍵を対応させて記憶する第2の共通鍵記憶手段と、前記認証依頼受信時、該認証依頼内のセッションIDと前記共通鍵を前記第2の共通鍵記憶手段に記憶させ、前記認証結果送信手段が前記認証結果を送信する時、前記セッションIDと共通鍵を前記第2の共通鍵記憶手段から削除する再送検出手段を更に備えることを特徴とする請求項1乃至4のいずれか1つに記載の認証システム。

【請求項6】 前記認証対象となっているクライアントは、前記認証サーバからパスワードの要求があった時、該パスワードと共に自己が記憶しているセッションIDを前記認証サーバに送信し、前記再送検出手段は、前記クライアントから受信したセッションIDにより前記第2の共通鍵記憶手段を検索して再送を検出することを特徴とする請求項5に記載の認証システム。

【請求項7】 前記アプリケーションサーバ及び認証サ

サーバは、前記第1及び第2の共通鍵記憶手段にセッションID及び共通鍵を記憶してから特定時間経過に該セッションID及び共通鍵を削除するタイムアウト手段を更に備えることを特徴とする請求項5又は6に記載の認証システム。

【請求項8】 前記認証依頼送信手段及び前記認証結果送信手段は、HTTPのリダイレクト機能により、認証対象となっているユーザのクライアントを経由して認証サーバまたはアプリケーションサーバに認証依頼または認証結果を送信することを特徴とする請求項2乃至7のいずれか1つに記載の認証システム。

【請求項9】 前記認証対象となっているクライアントは、前記アプリケーションサーバから前記認証依頼を受信すると該認証依頼にユーザのデジタル証明書を加して前記認証サーバに送信することを特徴とする請求項1乃至8に記載の認証システム。

【請求項10】 前記パスワード取得手段は、前記認証対象となっているユーザのクライアントに前記デジタル証明書内のユーザIDと共にパスワード要求を送信することを特徴とする請求項9に記載の認証システム。

【請求項11】 クライアントと、認証されたユーザにサービスを提供するアプリケーションサーバと、該アプリケーションサーバからの認証依頼に対してユーザの認証を行う認証サーバとがネットワークで接続されているシステムに於けるユーザ認証方法であって、前記アプリケーションサーバは、前記認証依頼を前記クライアントを介して前記認証サーバに行い、前記認証サーバは、前記認証依頼に対する認証結果を前記クライアントを介して前記アプリケーションサーバに送ることを特徴とするユーザ認証方法。

【請求項12】 前記アプリケーションサーバは、前記認証依頼に認証対象であるユーザのクライアントの固有の情報を含めることを特徴とする請求項11に記載のユーザ認証方法。

【請求項13】 前記アプリケーションサーバは、前記認証依頼に前記クライアントからのアクセス日時に基づく日時情報を含め、前記認証サーバは前記日時情報と現在の日時を比較することを特徴とする請求項11又は12に記載のユーザ認証方法。

【請求項14】 前記アプリケーションサーバは、前記ユーザからのログインに対してユニークなIDを生成し、該IDをキーとするテーブルに前記認証依頼の暗号化に用いた共通鍵を登録することを特徴とする請求項10乃至13のいずれか1つに記載のユーザ認証方法。

【請求項15】 前記テーブルに前記共通鍵を登録してから一定期間経過後、該共通鍵を削除することを特徴とする請求項14に記載のユーザ認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、アプリケーション

のクライアント／サーバと認証サーバによって構成され、これらをネットワークで接続するシステムにおける、公開鍵暗号方式を用いた認証システム及び認証方法に関する。

【0002】

【従来の技術】インターネットの発達によりネットワークを介した様々なサービスの提供や電子商取引が盛んになっている。この為、ネットワークを介してやり取りされるデータの機密性を確保することや、またデータが第三者によって改ざんされていないことを確認し、データの正当性、安全性を確保するための認証技術が重要になっている。

【0003】現在一般的に行われている認証サーバを用いたユーザ認証方式を図6に示す。

【0004】図6の構成では、ネットワークを介してクライアント103にサービスを提供するアプリケーションサーバ（以下APサーバという。尚以下の説明では、認証された特定ユーザに対してサービスを提供するサーバを総称してAPサーバという）101とAPサーバ101からの依頼により、ユーザの認証を行う認証サーバ102とがインターネットによって接続されている。また認証サーバ102では、ユーザIDとパスワードをテーブル104（以下、IDテーブルという）にデータベース化して登録して、一元管理している。

【0005】以下に図6を用いて従来の認証方式での動作を説明する。尚下記の説明中での(01)～(04)の番号は図6内の番号と対応している。

【0006】クライアント103からユーザは、サービスを受けようとするAPサーバ101にネットワークを介してログインし、ユーザIDとパスワード（以下、アカウント情報という）を送信して、接続要求を行う（図6(01)）。

【0007】ユーザからの接続要求に対してAPサーバ101は、クライアント103から受取ったアカウント情報を暗号化して認証サーバ102に送信し、認証依頼を行う（(02)）。これを受けて認証サーバは、受信したアカウント情報を用いてIDテーブル104を照合して正当なユーザであるか否かを調べ、認証結果を暗号化してAPサーバ101に返信する（(03)）。

【0008】APサーバ101は認証サーバ102からの認証結果を元に、クライアント103に要求されているサービスを提供するアプリケーション画面もしくは認証エラー画面を送信する（(04)）。

【0009】一般に認証処理においては、ネットワークを介してやり取りされる情報を各コンピュータで暗号化してアカウント情報等の漏洩防止を行っており、その場合暗号化の方法としては以下のいずれかの方式を用いている。

【0010】(A) 共通鍵暗号方式

・送信側と受信側で固定の共通鍵を所有し、それを用い

て認証データを暗号／復号化する。

【0011】(B) 公開鍵暗号方式

・送信側は、認証データを受信側の公開鍵で暗号化して送信する。

・受信側は、送信されてきた認証データを自分の秘密鍵で復号化する。

【0012】(C) 共通鍵暗号方式と公開鍵暗号方式を組み合わせた方式。

・送信側は、ランダム生成した共通鍵を使って認証データを暗号化し、その共通鍵を受信側の公開鍵で暗号化（以下、デジタル封筒という）して暗号化した認証データと共に送信する。

・受信側は、自分の秘密鍵でデジタル封筒を復号化して共通鍵を取り出し、それを使って暗号化された認証データを復号化する。

【0013】尚(B)、(C) に関してはデジタル署名と組み合わせてデータの改ざん検出を行っている場合もある。

【0014】

【発明が解決しようとする課題】これまでの認証方式では、以下の様な問題点がある。

【0015】認証に用いられるパスワードは、氏名や個人情報から推測され易く、第三者に漏洩する危険性が高い。更に、APサーバ側にアカウント情報採取プログラムなどを組み込むことにより、APサーバがクライアントからアカウント情報を受信する過程において、認証に用いられるパスワード等のアカウント情報がAPサーバの管理者などに盗まれる可能性がある。

【0016】また本来利用資格が無い第三者（APサーバの管理者も含む）がネットワーク盗聴などによって認証データを傍受した場合、盗聴者がそのデータを再送することにより、正当なユーザに代わってアクセス権を奪うことが出来る。

【0017】本発明は上記問題を解消するためなされたものであり、ユーザIDやパスワード等のアカウント情報がAPサーバを経由せず認証を行うシステム及び認証方法を提供することを課題とする。また、ユーザやサーバの公開鍵証明書（以下、デジタル証明書という）をベースとした公開鍵暗号方式とパスワードを組み合わせた認証処理を行うシステムや認証方法を提供することを課題とする。

【0018】

【課題を解決するための手段】上記目的を達成するために、本発明による認証システムでは、クライアントと、認証されたユーザにサービスを提供するアプリケーションサーバ及びユーザの認証を行う認証サーバがネットワークで接続される認証システムにおいて、上記アプリケーションサーバは、第1の記憶手段、共通鍵生成手段、メッセージダイジェスト生成手段及び認証依頼送信手段を備える。

【0019】第1の記憶手段と、アプリケーションサーバの公開鍵、アプリケーションサーバの秘密鍵及び認証サーバの公開鍵を記憶する。

【0020】共通鍵生成手段は、共通鍵を生成する。

【0021】メッセージダイジェスト生成手段は、認証対象となっているユーザのクライアントからの接続要求に対し、該クライアントの固有情報を含む認証要求メッセージ及び該認証要求メッセージのメッセージダイジェストを生成する。

【0022】認証依頼送信手段は、上記メッセージを上記共通鍵で、上記メッセージダイジェストを上記アプリケーションサーバの秘密鍵で、及び上記共通鍵を上記認証サーバの公開鍵で暗号化し、これらを認証依頼として上記認証対象となっているユーザのクライアントを介して上記認証サーバに送信する。

【0023】また上記認証サーバは、第2の記憶手段、共通鍵復号化手段、復号化手段及び認証依頼改ざん検出手段を備える。

【0024】第2の記憶手段、認証サーバの公開鍵、認証サーバの秘密鍵及びアプリケーションサーバの公開鍵を記憶する

共通鍵復号化手段は、上記認証対象となっているユーザのクライアントを介して受信した上記認証依頼のうち、上記共通鍵を上記認証サーバの秘密鍵で復号化する。

【0025】復号化手段は、上記認証依頼のうち、上記共通鍵復号化手段が復号化した共通鍵で上記認証要求メッセージを、及び上記アプリケーションサーバの公開鍵で上記メッセージダイジェストを復号化する。

【0026】認証依頼改ざん検出手段は、上記復号化手段が復号化した認証要求メッセージから生成したメッセージダイジェストと、上記復号化手段が復号化したメッセージダイジェストを比較して上記認証依頼の改ざんを検出する。

【0027】また上記認証サーバは、ユーザIDとパスワードを対応させて記憶するアカウント情報記憶手段と、上記改ざん検出手段が上記認証依頼が改ざんされていないと認定した時、上記認証対象となっているユーザのクライアントにパスワードを要求し、該クライアントからパスワードを得るパスワード取得手段と、上記認証要求内のユーザIDと上記パスワード取得手段が取得したパスワードの組合わせが上記アカウント情報記憶手段に記憶されていれば、認証結果として上記ユーザを認証することを示す情報を生成し、該認証結果を含む認証応答メッセージを上記認証依頼に対する応答として上記認証対象となっているユーザのクライアントを介して上記アプリケーションサーバに送信する認証結果送信手段とを更に備える構成とすることも出来る。

【0028】更に認証サーバは上記認証結果送信手段が、上記認証応答メッセージのメッセージダイジェストを生成し、上記認証応答メッセージを上記共通鍵で、及

び上記メッセージダイジェストを上記認証サーバの秘密鍵で暗号化して、これらを上記認証依頼に対する応答として上記認証対象となっているユーザのクライアントを介して上記アプリケーションサーバに送信する構成とする。そして、上記アプリケーションサーバが、受信した暗号化された上記認証応答メッセージを上記共通鍵で、及び上記メッセージダイジェストを上記認証サーバの公開鍵で復号化する認証応答復号化手段と、上記認証応答復号化手段が復号化したメッセージダイジェストと、上記認証応答復号化手段が復号化した上記認証応答メッセージから生成したメッセージダイジェストとを比較して上記認証結果メッセージの改ざんを検出する認証依頼改ざん検出手段を更に備える構成とすることも出来る。

【0029】本発明によれば、アカウント情報はアプリケーションサーバを経由せず、アプリケーションサーバと認証サーバとの認証処理時のやり取りは全て認証対象となっているユーザのクライアントを経由して行われるので、第三者によってアカウント情報が盗まれにくい。また成りすましを目的とする認証データの再送に対して共通鍵を第1又は第2の共通鍵登録手段に登録しておくことにより検出することが出来る。

【0030】

【発明の実施の形態】以下、本発明を図面に基づいて説明する。

【0031】図1は、本実施形態における構成を示す図である。

【0032】図1の構成では、ユーザ端末となる複数のクライアント3とネットワークを介してクライアント3にサービスを提供する1乃至複数のAPサーバ1及びAPサーバ1からの依頼によりユーザの認証を行う認証サーバ2とによって構成され、これらはインターネット技術を基板として構築されたネットワークによって接続されている。

【0033】APサーバ1及び認証サーバ2は、自己の秘密鍵と公開鍵、自己及び互いのデジタル証明書を記憶している。尚このAPサーバ1のデジタル証明書、認証サーバ2のデジタル証明書及び後述するユーザのデジタル証明書は認証サーバ2が発行したものでも公的認証局が発行したものでもよい。

【0034】認証サーバ2はIDテーブル21を備え、このIDテーブル21にユーザ認証用にアカウント情報の組み合わせをデータベース化して登録して、一元管理している。またAPサーバ1及び認証サーバ2は、後述する認証要求メッセージの暗号化に用いる共通鍵を登録しておく共通鍵テーブル11、22を備えている。更に認証処理が中断した場合などの理由で、セッションIDと共通鍵の情報が共通鍵テーブル11、22中に保存されたままとなることを防ぐため、共通鍵を保存後一定時間後に共通鍵の情報を共通鍵テーブル11、22から削除

する不図示のタイムアウトプログラム12、23を備えている。

【0035】図1のシステムでは、認証処理において、認証の依頼や認証結果の返信等のAPサーバ1と認証サーバ2との間の認証データのやり取りにHTTP(hypertext transfer protocol)プロトコルなどに実装されている別サーバに自動的に接続するリダイレクト機能を用い、APサーバ1と認証サーバ2とで直接やり取りせず、クライアント3を経由して行うことを特徴としている。従って、アカウント情報がAPサーバ1に送られないので、APサーバ1側からパスワード等のアカウント情報が漏洩することはない。

【0036】図2から図5は、認証処理における通信手順を説明したものである。以下に、図面を参照して順を追って説明する。尚下記の説明中での(1)～(15)の番号は各認証処理を示すもので、図2乃至図4内の番号と対応している。

【0037】図2は、図1のシステムによる認証処理のうち、ユーザがクライアント3からAPサーバ1にログインし、APサーバ1が認証サーバ2にそのユーザの認証を依頼するまでの処理の流れを詳細に示したものである。尚下記の説明中での(1)～(6)の番号は図2中の番号と対応している。

【0038】まずサービスを受けようとするユーザは、クライアント3からネットワークを介してAPサーバ1にログインして接続要求を行う(1)。この際、クライアント3はIPアドレスなどのクライアント固有の情報(以下クライアント固有情報という)をAPサーバ1に送信する。

【0039】APサーバ1では、クライアント3からの接続要求に対して、認証サーバ2にこのユーザの認証の依頼を行う認証通信データ(i)を生成し(2)、これをクライアント3に返信する(3)。

【0040】図3は、APサーバ1で行われる通信データ(i)の生成の流れを示す図である。

【0041】APサーバ1では、クライアント3がログインすると、セッションIDを生成する。このセッションIDは、APサーバ1に設定されるセッションを一意に識別する識別子で例えば接続要求を受け付けた時刻などを元にして生成したユニークな文字列を用いてもよいし、或は接続要求が有った順に順次符号を割付けてもよい。

【0042】次にAPサーバ1は、このセッションID、アクセス日時、クライアント固有情報、及びAPサーバ名、URLなどのAPサーバ固有の情報からなる認証要求メッセージを生成する。そしてこの認証要求メッセージに対し、ハッシュ関数を用いてメッセージダイジェストを生成し、これをAPサーバ1の秘密鍵で暗号化してデジタル署名とする。また認証要求メッセージをランダム生成した共通鍵を使って暗号化する。この共通鍵は

APサーバ1のメモリ、ハードディスクまたはICカードなどの記憶媒体上に作成した、セッションIDをキーとした共通鍵テーブル11に保存する。この時に、認証処理が中断した場合などの理由で、セッションIDと共通鍵の情報がAPサーバ1の記憶媒体中に保存されたままとなることを回避するため、ある一定時間後に共通鍵テーブル11から共通鍵の情報を削除する不図示のタイムアウトプログラム12を起動する。

【0043】次に認証サーバのデジタル証明書内の認証サーバ2の公開鍵で、認証要求メッセージの暗号化に用いた共通鍵を暗号化してデジタル封筒を生成する。

【0044】そしてAPサーバ1は、これらのデータのうちセッションIDをクッキーとして、また暗号化した認証要求メッセージとそのデジタル署名及びデジタル封筒をURL付加情報として、認証サーバ2へのリダイレクト命令を設定した通信ヘッダデータと一緒にクライアント3に通信データ(i)として送信する(3)。この様に本実施形態では、WWW(World Wide Web)のクッキー技術により、セッションIDはクライアント3側の記憶媒体に保存されるので、セッションIDがどのクライアントに対して発行されたものかを示す情報をAPサーバ1では管理していない。従って、第三者に共通鍵テーブル11の内容を盗まれてもこれから認証対象のユーザを特定することは出来ない。

【0045】通信データ(i)をAPサーバ1から受信すると、クライアント3ではクッキーとして送信されたセッションIDがクライアント3のメモリ等の記憶媒体に保存される。またクライアント1は、通信データ(i)のヘッダのリダイレクト命令に従い、HTTPプロトコルなどに実装されているリダイレクト機能により認証サーバ2に接続する。そして、通信データ(i)のURL付加情報として送信されてきた暗号化された認証要求メッセージとそのデジタル署名及びデジタル封筒に加え、クライアント3が持つユーザのデジタル証明書とクライアント3のクライアント固有情報をSSL(Secure Socket Layer)などによる暗号方式を用いて暗号化して通信データ(ii)を生成し(4)、これを認証サーバ2に送信する(5)。

【0046】通信データ(ii)を受信した認証サーバ2では、改ざんの検出等この通信データ(ii)そのものの信頼性に対する検証を行う(6)。

【0047】認証サーバ2では、まずユーザのデジタル証明書内に含まれる有効期限や発行元などの情報を元に、このデジタル証明書が有効なものであるか検証を行う。これによって認証対象のユーザが正式なユーザかどうか判別が行える。

【0048】次に、デジタル封筒を認証サーバ2の秘密鍵で復号化し、認証要求メッセージの暗号化に用いた共通鍵を取り出す。そしてこの共通鍵で暗号化された認証要求メッセージを復号化し、クライアント固有情報や

APサーバ名、URLなどのAPサーバ固有の情報、アクセス日時、セッションIDを得る。また共通鍵はセッションIDを検索キーとして共通鍵テーブル22に保存する。

【0049】次にデジタル署名をAPサーバのデジタル証明書内のAPサーバ1の公開鍵で復号化して認証要求メッセージのメッセージダイジェストを取り出す。そして、これを先に復号化した認証要求メッセージに対してAPサーバ1と同じハッシュ関数を用いて生成したメッセージダイジェストと比較して、両者が一致しなければ、受信データはAPサーバ1から送信された認証データが認証サーバ2に届くまでの(3)から(5)の過程で改ざんされていることとなる。この様に暗号化されて送信されてきた認証要求メッセージから生成したメッセージダイジェストと、送信前に送信元であるAPサーバ1で(過程(2)で)生成されたメッセージダイジェストを比較することによって、途中で送信データの改ざんが行われていないかを判別することが出来る。

【0050】デジタル署名を復号化したメッセージダイジェストと、認証要求メッセージから生成したメッセージダイジェストが一致したら、認証サーバ2では、次に共通鍵により復号化した認証要求メッセージからクライアント3固有の情報を取り出し、これを(4)の過程で生成されたクライアント3の固有情報と照合し、通信データ(ii)が別のクライアント3から偽って送信したものでないか判別する。また復号化した認証要求メッセージからアクセス日時(2)の過程で生成)を取り出し、これを現在の日時と比較する。これにより過去の認証で用いた古い通信データ(ii)を同じクライアント3から再送していないか判別する。なおこの時APサーバ1と認証サーバ2の基準となる時刻にずれが生じている場合があるので、ある程度の時刻に差があっても問題なしとする。またこの時に、認証処理が中断した場合などの理由で、セッションIDと共通鍵の情報がAPサーバ1の記憶媒体中に保存されたままとなることを回避するため、ある一定時間後に共通鍵テーブル22から共通鍵の情報を削除する不図示のタイムアウトプログラム23を起動する。

【0051】図4は図1のシステムによる認証処理のうち、認証サーバ2が通信データ(ii)を受信後、認証サーバ2とクライアント3の間での処理の流れを詳細に示した図である。下記の説明中での(7)～(9)の番号は図4中の番号と対応している。

【0052】上記(6)の過程の各検証で、認証サーバ2が受信した通信データ(ii)に改ざん等が検出されず信頼がおけるものと認定されれば、次に認証サーバ2はこの通信データ(ii)から得たデータを用いてクライアント3上のユーザに対するユーザ認証を行う。

【0053】まず認証サーバ2は、クライアント3に対してパスワード入力のためのログイン画面のデータをSSLなどによる暗号方式を用いて送信し、パスワードの

入力を要求する(7))。この際、ユーザ証明書に含まれていたユーザIDを用いて、ログイン画面には既にユーザIDを入力済みの状態として送信する。これにより、ユーザはユーザIDを入力する手間が省ける。

【0054】このデータが送信されクライアント3側にログイン画面が表示されると、ユーザは画面上からユーザ認証のためのパスワードを入力し、記憶媒体中にクッキーとして保存されているセッションIDと共にSSLなどの暗号方式を用いて認証サーバ2に送信する(9))。

【0055】認証サーバ2では、クライアント3から受信したセッションIDを検索キーとして共通鍵テーブル2を検索し、対応する共通鍵が共通鍵テーブル2に登録されているかどうかを検証する。これにより、現在認証処理中の通信であることを判別出来、このセッションIDとパスワードが認証対象としているユーザ以外から送信されたものでないことを確認する。

【0056】次に認証サーバ2は、クライアント3から受信したパスワードとユーザIDを元にIDテーブル2を照合し、認証対象となっているユーザが正当なユーザであるかを判別する。その結果、クライアント3から送信されてきたユーザID及びパスワードと同じ組み合わせのものがIDテーブル2に登録されていれば、このユーザは正当なユーザであるとして認証許可し、逆に対応するものがIDテーブル2に登録されていなければ再度ログイン画面のデータをクライアント3に送信してパスワードの入力を求める。

【0057】図5は、図1のシステムによる認証処理のうち、クライアント3からパスワードを認証サーバ2へ送信後の処理の流れを詳細に示した図である。以下の説明中での(10)～(16)の番号は図5中の番号と対応している。

【0058】ユーザに対する認証が終了すると認証サーバ2は、認証結果をAPサーバ1に通知する通信データ(iii)を生成し(10)、クライアント3に送信する(11))。

【0059】認証サーバ2による通信データ(iii)の生成は以下の様にして行われる。

【0060】まず認証サーバ2は、上記した種々の検証結果に基づいた、ユーザに対する認証結果及びユーザ情報等からなる認証応答メッセージを生成する。そしてこの認証応答メッセージのメッセージダイジェストをハッシュ関数により生成し、これを認証サーバ2の秘密鍵で暗号化してデジタル署名を生成する。また共通鍵テーブル2に登録しておいた共通鍵を用いて認証応答メッセージを暗号化する。そしてこの暗号化した認証応答メッセージとそのデジタル署名をURL付加情報とし、通信ヘッダ部分にAPサーバ1へのリダイレクト命令を設定した通信データ(iii)として生成し、これをクライアント3に送信する。

【0061】また通信データ(iii)の送信後、この認証処理に用いた共通鍵を共通鍵テーブル2から削除する。これにより、以降第三者の成りすまし等によって同じ共通鍵による通信データ(ii)がクライアント3から再送されてきても、これによって正当なユーザとして認証してしまうことはない。

【0062】この通信データ(iii)を受信するとクライアント3は、そのヘッダ部分のリダイレクト命令に従ってAPサーバ1に接続する(12))。そして通信データ(iii)に付加している暗号化された認証応答メッセージ及びそのデジタル署名と共に自己の記憶媒体にクッキーとして記憶しているセッションIDを通信データ(iv)としてAPサーバ1に送信する(13))。

【0063】クライアント3から通信データ(iv)を受信すると、APサーバ1はこの通信データ(iv)内の認証サーバ2による認証結果に基づいて、ユーザを認証するかどうかを決める(14))。

【0064】APサーバ1では、受信した通信データ(iv)から以下の様にして正当なユーザとして認証するかどうかの判断を行う。

【0065】まず、通信データ(iv)内のセッションIDを用いて共通鍵テーブル1を検索し、対応する共通鍵が共通鍵テーブル1に登録されているか調べる。この結果、共通鍵テーブル1に対応するセッションIDと共通鍵の組み合わせが登録されていればまだ認証処理が完了していないユーザについての認証結果を含む通信データ(iv)であると判断出来、また対応するものが共通鍵テーブル1に登録されていなければ、第三者がなり代わりを目的として古い通信データ通信データ(iv)を再送してきたものと判断することが出来る。

【0066】次に共通鍵テーブル1より取り出した共通鍵で暗号化された認証応答メッセージを復号化する。またデジタル署名を認証サーバ2の公開鍵で復号化し、先に復号化した認証要求メッセージのメッセージダイジェストと比較し、(11)から(13)の過程で内容が改ざんされていないかを判別する。

【0067】上記した検証で問題が無ければ、受信した通信データ(iv)内に格納されている認証サーバ2による認証結果は正当なものであるので、APサーバ1は、復号化した認証応答メッセージより認証サーバ2による認証結果を取り出し、この認証結果がユーザを認証することを示すものであればユーザから要求のあるサービスに対応するアプリケーション画面を、またユーザを認証しないことを示すものであればユーザが認証されなかったことを通知するエラー画面のデータをクライアント3に送信する(15))。又この時、クライアントに送信するデータに、クライアント3にクッキーとして保存しておいたセッションIDを消去する命令を通信ヘッダに設定しておく。

【0068】この送信処理後、APサーバ1は、暗号化

に用いた共通鍵を共通鍵テーブル11より消去し、以降同一の通信データ(iv)がクライアント3から再送されてもこれによりユーザを認証することがないようにする。

【0069】APサーバ1からアプリケーション画面若しくはエラー画面のデータを受信したクライアントは、これを画面表示すると共に、自己の記憶媒体の中にクッキーとして保存されているセッションIDを削除する。

【0070】この様に本実施形態のシステムでは、ユーザのアカウント情報は、一切APサーバ1には送信されない。この為、第三者が、APサーバ1に何等かの仕掛けを行っても、アカウント情報をてに入れることは出来ない。また、認証の為の情報のやり取りは、全て認証対象となっているユーザの端末であるクライアント3を介して行うこととなる。よって、盗聴を行う場合は、セキュリティレベルの高い認証サーバ2や特定が困難なクライアント3に対して非常に困難である。更にAPサーバ1及び認証サーバ2では、認証処理時に各自の共通鍵テーブル11、22のチェックを行うので、第三者による過去の通信データを再送に対しても対応することが出来る。

【0071】

【発明の効果】以上説明したように、本発明による認証システムを用いれば、認証処理時にやり取りされるユーザIDやパスワード等のアカウント情報はAPサーバを経由しないので、たとえAPサーバ側でデータの漏洩やネットワーク盗聴が行われても、第三者にアカウント情報が洩れることは無い。

【0072】またユーザ認証にデジタル証明書を用いることができるので、より高い認証レベルを実現するこ

とが出来る。

【0073】更には、認証処理時に共通鍵を生成してこれを登録しておき、認証処理完了後これを削除するので、第三者による成りすましを目的とした認証データの再送に対しても対応することが出来る。

【0074】また認証処理時に、ユーザがユーザIDの入力を不要とする構成とすることが出来、ユーザの負荷軽減することが出来る。

【図面の簡単な説明】

【図1】本実施形態に於けるシステム構成を示す図である。

【図2】ユーザがログインしてから、APサーバが認証サーバに認証を依頼するまでの処理の流れを詳細に示した図である。

【図3】APサーバで行われる通信データ(i)の生成の流れを示す図である。

【図4】通信データ(ii)を受信後、認証サーバとクライアントの間で行われる処理の流れを詳細に示した図である。

【図5】クライアントからパスワードを認証サーバへ送信後の処理の流れ詳細に示した図である。

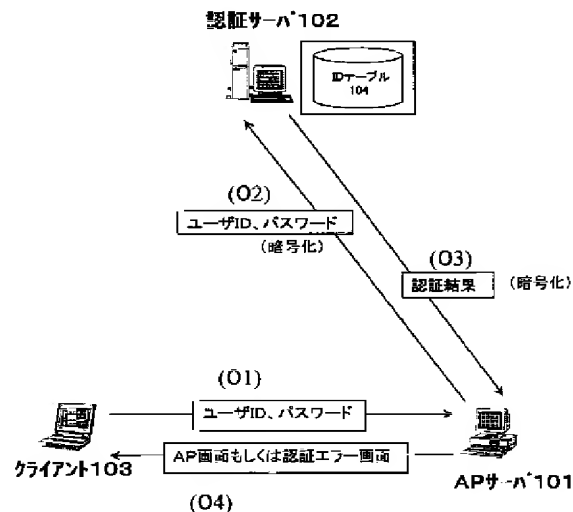
【図6】一般的に行われている認証サーバを用いたユーザ認証方式を示す図である。

【符号の説明】

- 1、101 APサーバ
- 2、102 認証サーバ
- 3、103 クライアント
- 11、22 共通鍵テーブル
- 21、104 IDテーブル

【図6】

一般的に行われている認証サーバを用いた
ユーザ認証方式を示す図



【図5】

クライアントからパスワードを認証サーバへ
送信後の処理の流れを詳細に示した図

